



**INFORMATIK-BIBER SCHWEIZ  
CASTOR INFORMATIQUE SUISSE  
CASTORO INFORMATICO SVIZZERA**

# ICT-V Tagung der PHBern

31.10.2015

Workshop von Alain Geering

[www.medien-bildung.ch](http://www.medien-bildung.ch)



**INFORMATIK-BIBER SCHWEIZ  
CASTOR INFORMATIQUE SUISSE  
CASTORO INFORMATICO SVIZZERA**

# Übersicht

- Informatik-Biber Wettbewerb
- Informatik-Biber Module
- Praxis-Bericht
- Test
- Individuelle Vertiefung
- Fragen / Diskussion



# Informatik-Biber Wettbewerb

- 3. – 13. Klasse (8 – 20 Jahre)
- erstmals 2010 in der Schweiz
- 2015: 9. – 13. November
- 2014: 10'500 Teilnehmende
- online Wettbewerb, ca. 40 Min
- weckt Interesse an Informatik
- ohne Vorkenntnisse möglich
- Preisverleihung am edu-i-day
- Vorbereitung: alle Fragen der letzten Wettbewerbe vorhanden (über 100)

# LP 21

- Kampf der Ideologien
- Kompetenzbereich

Medien	Schülerinnen und Schüler können an der Mediengesellschaft selbstbestimmt, kreativ und mündig teilhaben und sich sachgerecht und sozial verantwortlich verhalten.
Informatik	Schülerinnen und Schüler verstehen Grundkonzepte der automatisierten Informationsverarbeitung, nutzen sie zur Entwicklung von Lösungsstrategien in allen Lebensbereichen und zum Verständnis der Informationsgesellschaft.
Anwendungskompetenzen	Schülerinnen und Schüler nutzen Informations- und Kommunikationstechnologien in allen Fach- und Lebensbereichen effektiv und effizient.

# Material auf [www.informatik-biber.ch](http://www.informatik-biber.ch)

- Testwettbewerb
- Aufgabenarchiv aller Wettbewerbe (> 100)
- Lehrmittel Sekundarstufe 1: 6 Module
  - Lernfilm
  - Experimente, Aufgabenblätter, interaktive Aufgaben
  - Biber-Aufgaben;  
direkter Bezug zum Wettbewerb

# Lehrerkommentar

## Geheime Botschaften.

### Verschlüsseln – damit geheime Daten geheim bleiben

3

#### Umsetzungsvorschläge (bis 4 Lektionen)

4

Bildungsrelevanz des Themas gemäss Lehrplan 21

(aktuell diskutierte Vorarbeiten)

4

*Kompetenzbereiche des Fachbereichs „Mathematik“*

4

*Kompetenzbereiche des Fachbereichs „Natur, Mensch, Gesellschaft“*

4

Hintergrundwissen zur Verschlüsselung

5

*Terminologie*

5

*Verschiebechiffren*

6

*Monoalphabetische Chiffrierungen*

9

*Algorithmus: Statistische Analyse von Verschiebechiffren*

9

*Moderne monoalphabetische Algorithmen*

12

*Anmerkung zur Sicherheit im Internet*

13

*Monoalphabetische Chiffrierung natürlicher Sprachen ist unsicher*

13

#### Umsetzungshilfen

14

Reflexion Lernfilm / Perspektiven der Lernenden

14

Arbeitsblatt 1: „Botschaften verschlüsseln“

14

Arbeitsblatt 2: „Schlüssel erraten / Geheimcode knacken“

14

Arbeitsblatt 3: „Botschaften sicher verschlüsseln“

14

Informatik-Biberaufgaben zum Thema „Geheime Botschaften“

14

#### Mögliche Vertiefungen

15

Weiterführende Literatur

15

#### Lösungen

16

# Informatik-Biber Module

## Lehrmittel Sekundarstufe 1

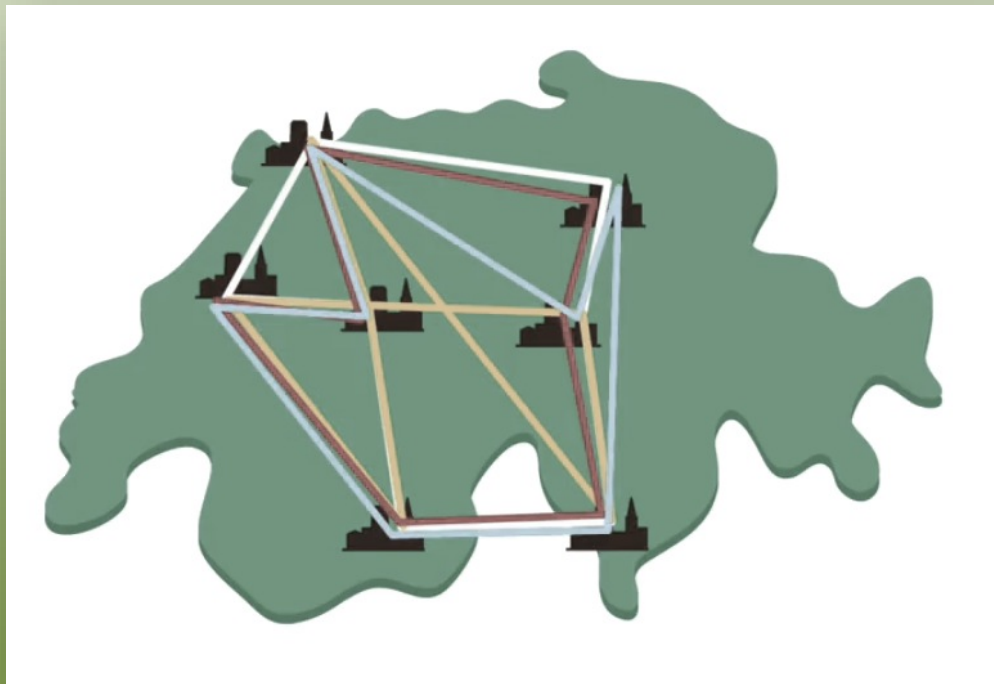
- Verkehr: Optimieren
- Musik: Komprimieren
- Geheime Botschaften: Verschlüsseln
- Internet: Routing
- Apps: Programmieren
- Auszeichnungssprachen: Beschreiben

# Informatik-Biber Module

## Lehrmittel Sekundarstufe 1

- Verkehr: Optimieren

### Travelling Salesman Problem



- optimalen Weg berechnen
- einfache, handlungsorientierte Experimente (Pausenplatz)
- leichter Einstieg (7. Klasse, sogar 5. / 6. Klasse)



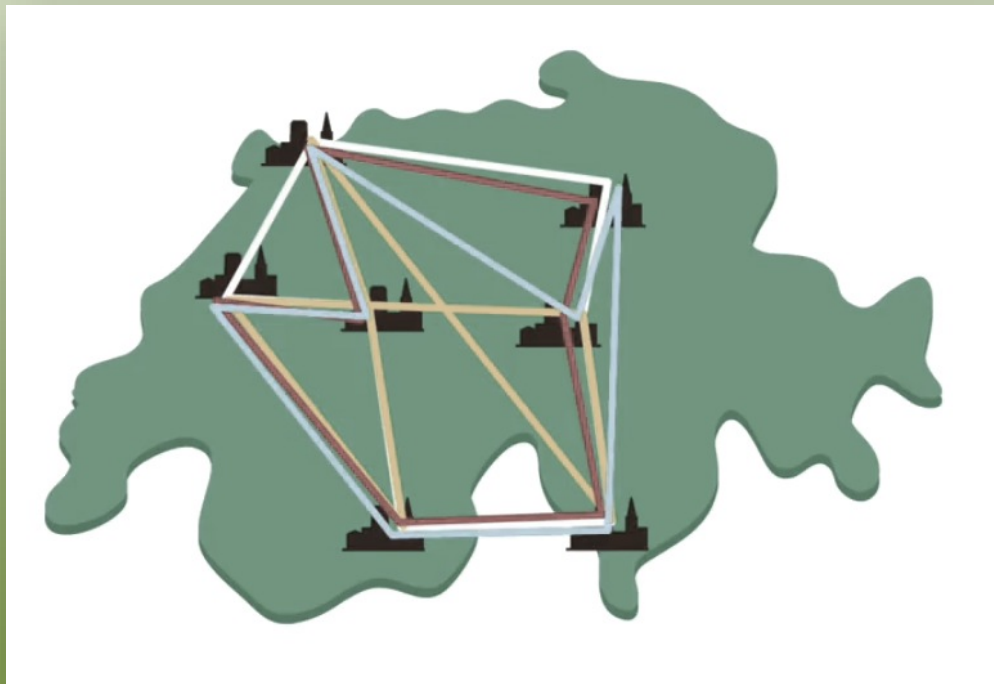


# Informatik-Biber Module

## Lehrmittel Sekundarstufe 1

- Verkehr: Optimieren

### Travelling Salesman Problem



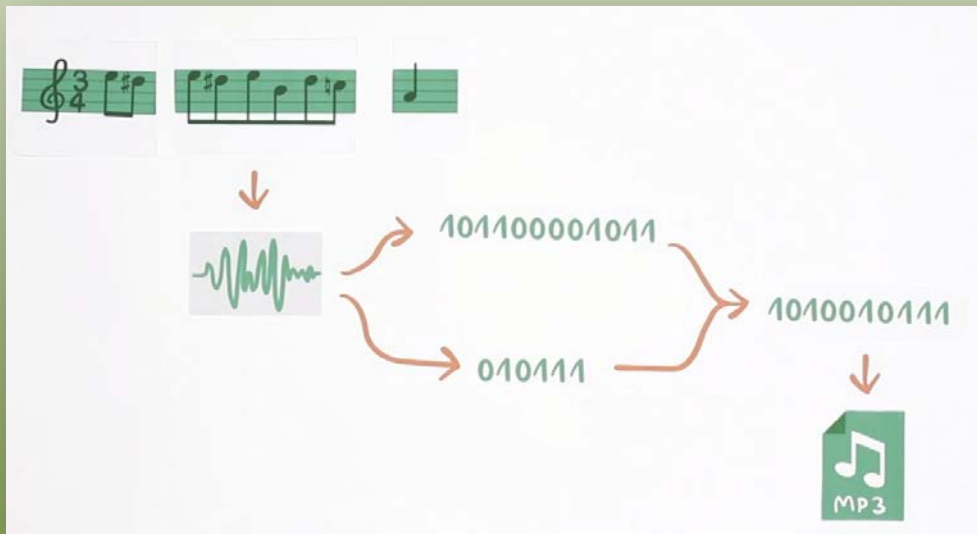
- Schweizer Geografie
- sparsamer Umgang mit Ressourcen
- Vertiefung Sek I: Formeln zur Berechnung von Möglichkeiten



# Informatik-Biber Module

## Lehrmittel Sekundarstufe 1

- Musik: Komprimieren



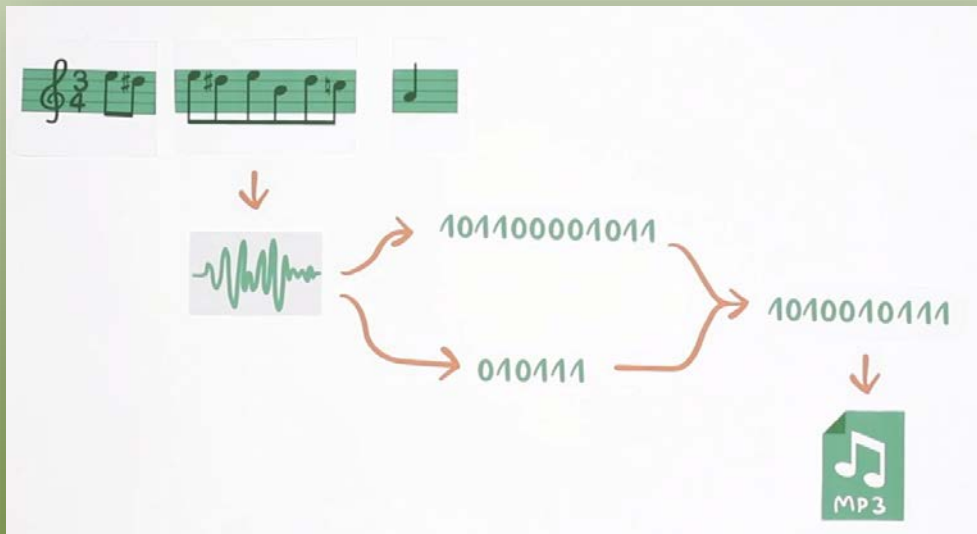
- direkter Bezug zu SchülerInnen
- eher 9. / 10. Schuljahr
- Abstrahierung: Daten = Zahlenfolgen
- Informatik-Terminologie  
Code, Bits, binär, ...



# Informatik-Biber Module

## Lehrmittel Sekundarstufe 1

- Musik: Komprimieren



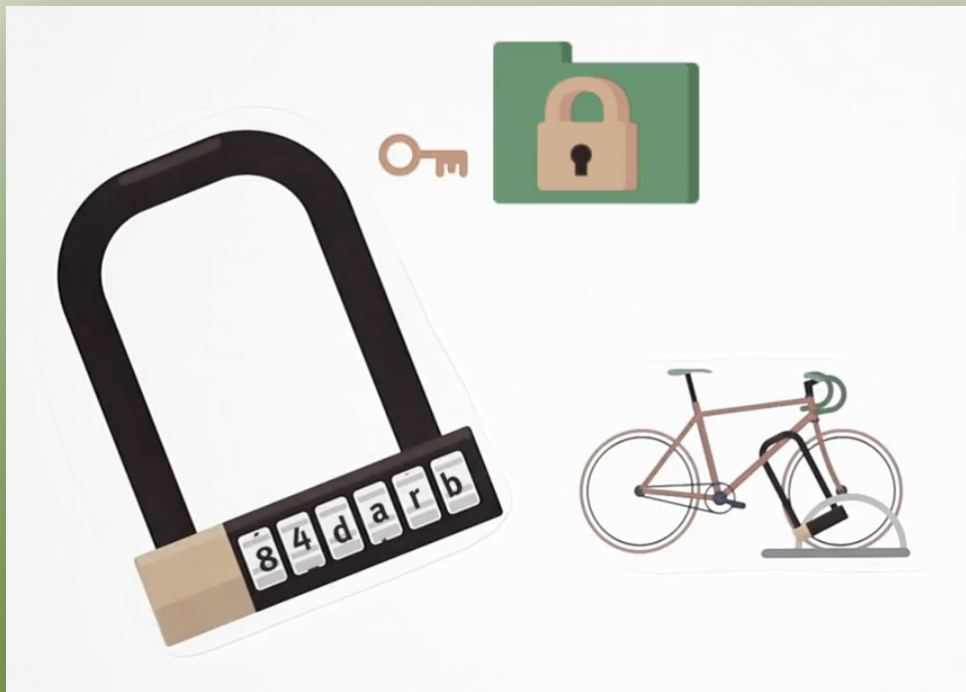
- Zahlensysteme
- technische Erfindungen
- Codierung
- Verweise auf Vertiefung für Mittelschulen



# Informatik-Biber Module

## Lehrmittel Sekundarstufe 1

- Geheime Botschaften: Verschlüsseln



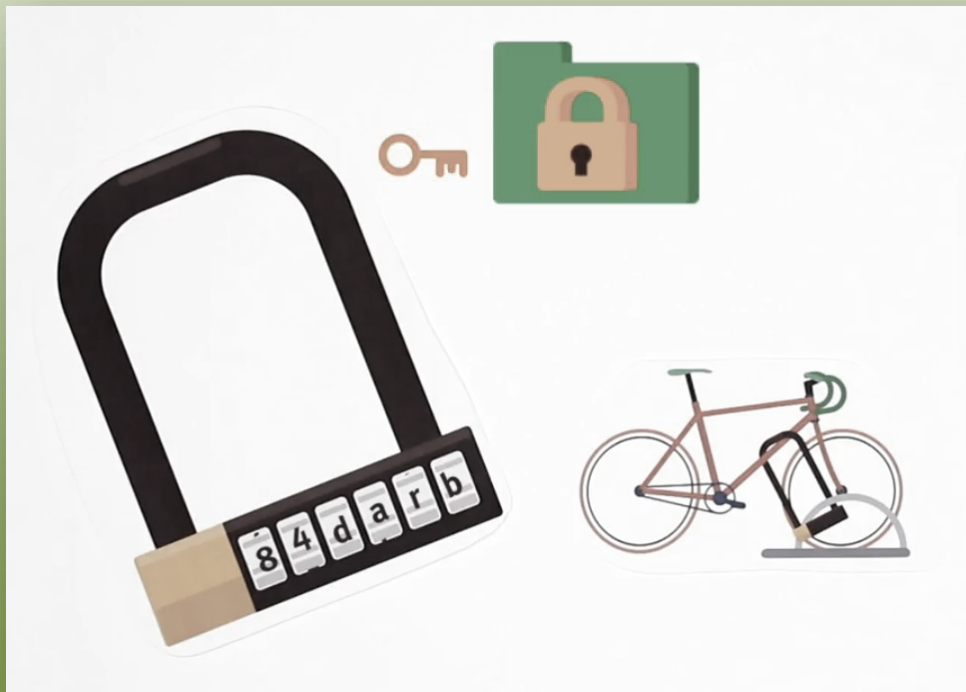
- spielerische Übungen
- Einstieg 7. Klasse
- konkret → abstrakt
- Chiffrierungsarten



# Informatik-Biber Module

## Lehrmittel Sekundarstufe 1

- Geheime Botschaften: Verschlüsseln



- Zahlenräume
- Diagramme
- Kombinatorik
- Prozentrechnen (Häufigkeit)
- technische Erfindungen



# Ziele des Informatik-Bibers

- zentrale Konzepte und Grundlagen der Informatik vermitteln
- ausgehend von Informatikgrundlagen Transfer zum modernen Alltag (Verkehr, Medizin, etc.) herstellen
- Berührungsängste zur Informatik abbauen
- Verständnis für die Funktionsweise des Computers

neu: [www.minibiber.ch](http://www.minibiber.ch)

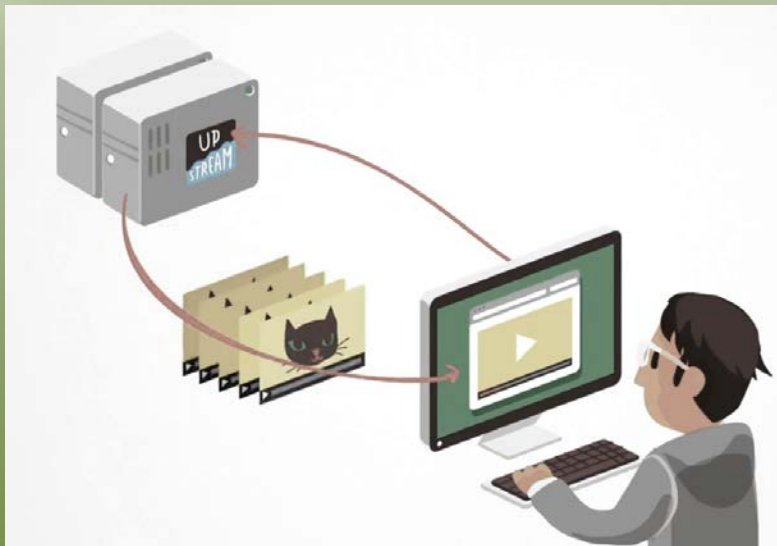
- Lehrplan 21
- v.a. Zyklus 1
- auch Zyklus 2 einsetzbar



# Informatik-Biber Module

## Lehrmittel Sekundarstufe 1

- Internet: Routing



- eher 9. / 10. Schuljahr
- Vorwissen:  
Binärsystem / E-Mail / Internet
- Terminologie:  
Netzwerk, Browser, Subnetze
- vorwiegend abstrakt





# Informatik-Biber Module

## Lehrmittel Sekundarstufe 1

- Internet: Routing

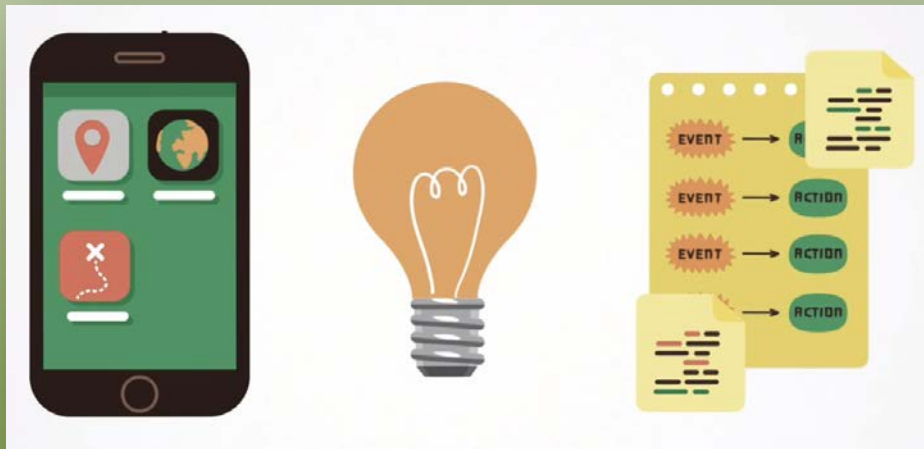
- Zahlensysteme
- technische Zusammenhänge



# Informatik-Biber Module

## Lehrmittel Sekundarstufe 1

- Apps: Programmieren



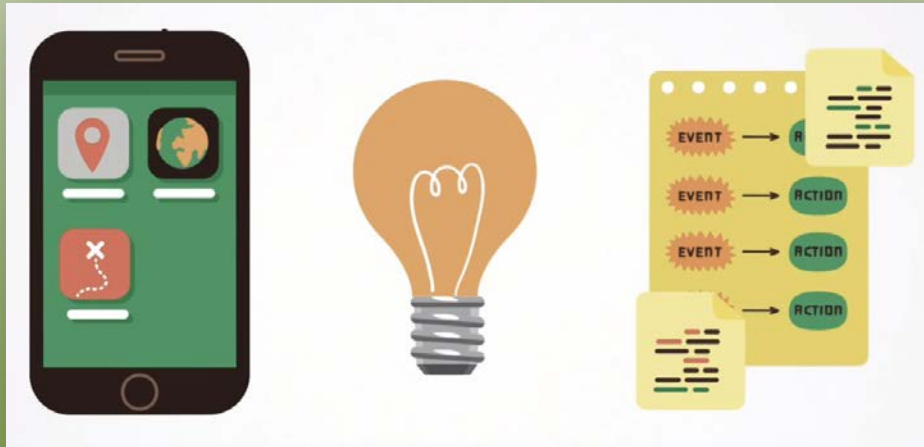
- konkretes Einstiegsbeispiel
- Apps: Alltag für SchülerInnen
- ab 7. Klasse auch tieferes Niveau
- wenig Vorwissen nötig
- einfache Programmierungs-Prinzipien



# Informatik-Biber Module

## Lehrmittel Sekundarstufe 1

- Apps: Programmieren



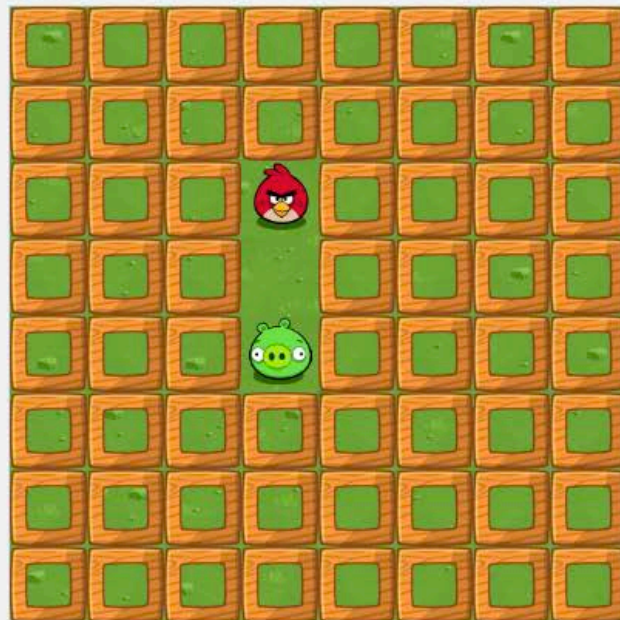
- spielerisches Programmieren
- Steigerung: Abstrahierung
- verschiedene Programmierungsumgebungen
- eigene App-Entwicklung



# Informatik-Biber Module

## Lehrmittel Sekundarstufe 1

- Apps: Programmieren



▶ Ausführen



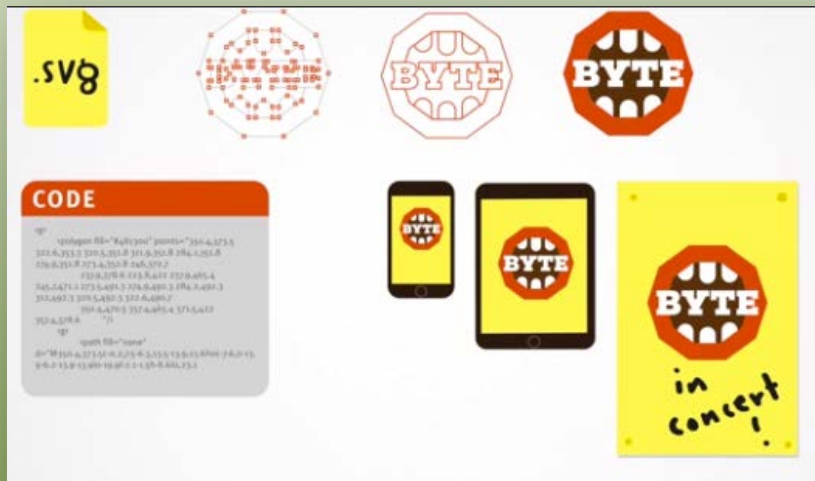
Kannst du mir helfen, das freche Schwein zu fangen? Stecke ein paar „vorwärts“-Bausteine zusammen und drücke „Ausführen“, um mir zu helfen.

Bausteine	Arbeitsbereich: 2 / 3 Blöcke	Neu beginnen	Programm anzeigen
<div>vorwärts bewegen</div> <div>nach links drehen ↺</div> <div>nach rechts drehen ↻</div>	<div>wenn ausführen</div> <div>vorwärts bewegen</div>		

# Informatik-Biber Module

## Lehrmittel Sekundarstufe 1

- Auszeichnungssprachen: Beschreiben



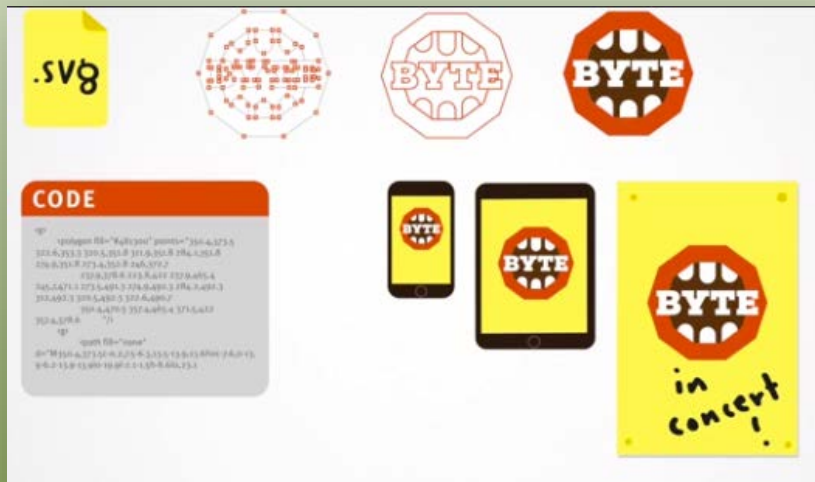
- konkrete Ausgangssituation
- einfach nachvollziehbar
- ab 7. Klasse
- praktischer Nutzen
- wenig Vorwissen nötig
- kreative Übungen (Logo-Gestaltung, Animation)



# Informatik-Biber Module

## Lehrmittel Sekundarstufe 1

- Auszeichnungssprachen: Beschreiben



- einfache, anwendbare Theorie
- erfolgversprechende Übungen
- Grundlagen Grafik / HTML
- einfaches Anwenden



# Informatik-Biber Module

## Lehrmittel Sekundarstufe 1

- Verkehr: Optimieren
- Musik: Komprimieren
- Geheime Botschaften: Verschlüsseln
- Internet: Routing
- Apps: Programmieren
- Auszeichnungssprachen: Beschreiben

# Informatik-Biber Module

## Lehrmittel Sekundarstufe 1

- Verkehr: Optimieren
- Musik: Komprimieren
- Geheime Botschaften: Verschlüsseln
- Internet: Routing
- Apps: Programmieren
- Auszeichnungssprachen: Beschreiben



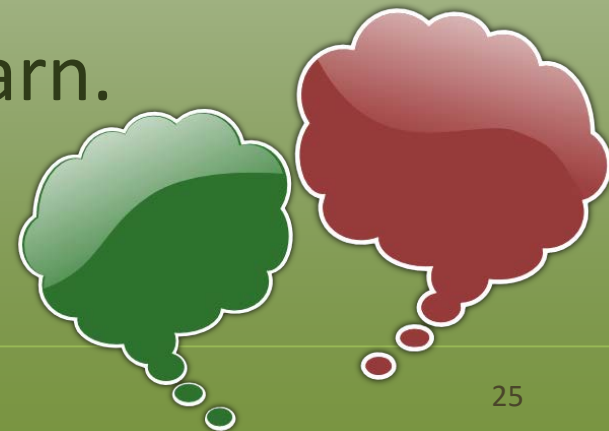
# Botschaften: Verschlüsseln

<http://informatik-biber.ch/geheimebotschaften/>

- Einstiegsfrage:

**Was wissen Schüler/innen über  
Verschlüsselungstechniken?**

Besprechen Sie sich 2 Minuten mit Ihrer  
Sitznachbarin / Ihrem Sitznachbarn.



INFORMATIK-BIBER SCHWEIZ  
CASTOR INFORMATIQUE SUISSE  
CASTORO INFORMATICO SVIZZERA

# Botschaften: Verschlüsseln

- Anknüpfungspunkte Alltag der Jugendlichen
  - ☐ Was für Informationen übermittelst du?
  - ☐ Welche Daten sind sensibel?
  - ☐ Wo verwendest du ein Passwort?
  - ☐ Wie wählst du dein Passwort?
  - ☐ Wo brauchst du einen Schlüssel?

**Inwiefern betreffen diese Themen die Jugendlichen?**





**facebook**  
Facebook for Windows Mobile

Email:

Password:

☒ Save Login



iCloud

Apple ID

Password

☐ Keep me signed in



# Botschaften: Verschlüsseln

- Lernfilm auf [www.informatik-biber.ch](http://www.informatik-biber.ch)

<https://youtu.be/ONVkrL7heRw>

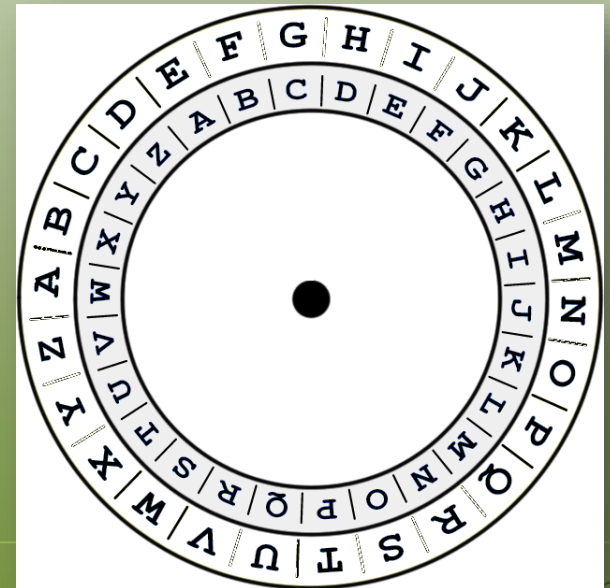
oder

<http://informatik-biber.ch/geheimebotschaften/>



# Botschaften: Verschlüsseln

- Unterrichtseinheit 7. Klasse Sek Sumiswald
  - **Einstiegsfrage**  
Wie kann man Daten verschlüsseln? - Gruppenarbeit
  - **Lernfilm**  
Informatik-Biber
  - **Chiffrierungen**  
Cäsar-Scheibe basteln,  
chiffrieren, dechiffrieren



ROT-X

links

rechts

1

&gt; Verschlüsseln

Entschlüsseln &lt;

Testen Sie Ihr Passwort		Mindestanforderungen
Passwort:	<input type="text"/>	<ul style="list-style-type: none"> <li>Mindestens 8 Zeichen</li> <li>Besteht mindestens aus 3 der 4 Gruppen:               <ul style="list-style-type: none"> <li>Großbuchstaben</li> <li>Kleinbuchstaben</li> <li>Zahlen</li> <li>Sonderzeichen</li> </ul> </li> </ul>
Ausblendung:	<input checked="" type="checkbox"/>	
Auswertung:	0%	
Komplexität:		

Aufwertungen		Bewertung	Anzahl	Punkte
✗	Anzahl der Zeichen	$+(n*4)$	0	0
✗	Großbuchstaben	$+\left((len-n)*2\right)$	0	0
✗	Kleinbuchstaben	$+\left((len-n)*2\right)$	0	0

— **Passwörter**  
Sicherheit  
Passwort-Check online

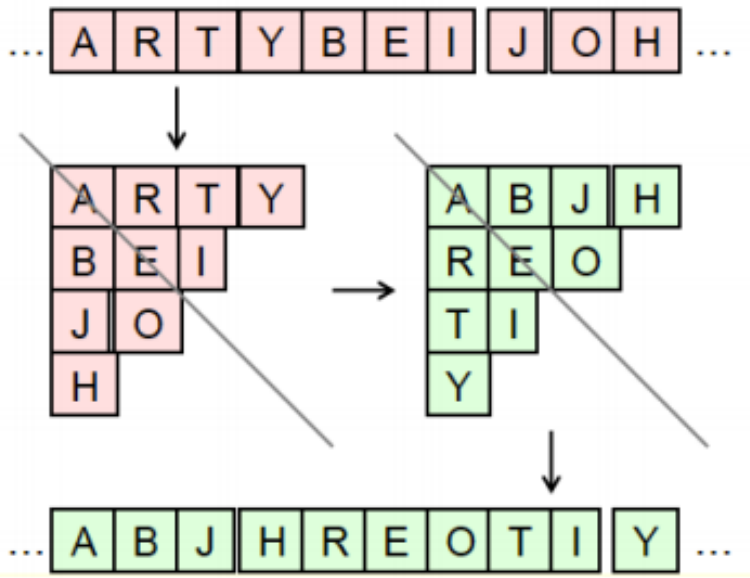


zweithäufigster Buchstabe: w = S  
Ez gEbssc hEcEz

# 27. Dreiecksverschleierung (SJ 7/8)

Betty möchte eine Nachricht an ihre beste Freundin schicken. Niemand sonst soll die Nachricht lesen können. Zuerst entfernt Betty alle Leerzeichen. Um den verbliebenen Text zu verschleiern, probiert sie das folgende Verfahren aus:

- 1. Der Text wird in Stücke eingeteilt, die 10 Zeichen (Buchstaben, Satzzeichen, ...) lang sind.
- 2. Jedes Textstück wird in Form eines Dreiecks aufgeschrieben (wie im Bild).
- 3. Das Dreieck wird an einer diagonalen Achse gespiegelt (wie im Bild).
- 4. Das Dreieck wird wieder als Textstück geschrieben (wie im Bild).



Die beste Freundin erhält von Betty einen verschleierten Text, der folgendes Textstück enthält: ASA?LKRLLE

**Wie lautet dieses Textstück im unverschleierten Text?**

# Testaufgabe

## Wettbewerb 2014

### 9. / 10. Klasse





## 2 Weltraumlabyrinth

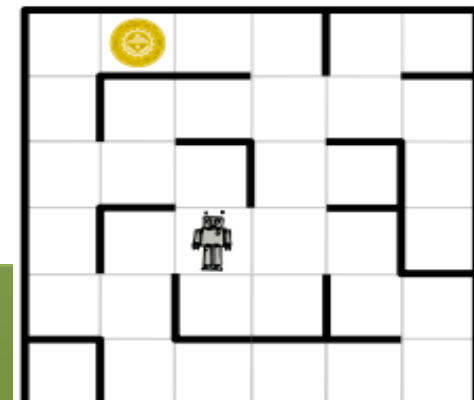
Raumfahrer sind auf einem verlassenen Planeten gelandet. Auf ihren Tele-Brillen sehen sie rätselhafte Bilder. Sie folgen den Signalen und machen als Quelle einen Roboter aus. Er steht in einem Labyrinth, das die Raumfahrer von ihrer erhöhten Position gut überblicken und sendet offensichtlich Nahaufnahmen seiner Umgebung.

Das Labyrinth ist in Quadrate eingeteilt. In einem davon befindet sich der Roboter. In einem anderen Quadrat befindet sich ein unbekanntes Objekt. Die Raumfahrer würden den Roboter gerne zum Objekt steuern, um Nahaufnahmen davon zu sehen.

Plötzlich flimmern vier kryptische Textzeilen mit insgesamt vier verschiedenen Wörtern über die Tele-Brillen. Auch der Roboter und das Objekt sind zu erkennen. Nach einigem Grübeln vermuten die Raumfahrer: Die vier Wörter sind Befehle, die den Roboter jeweils in ein benachbartes Quadrat steuern; für jede der vier möglichen Richtungen gibt es einen eigenen Befehl. Ausserdem sind die Raumfahrer sicher, dass eine der Textzeilen eine Befehlsfolge ist, die den Roboter zum Objekt steuert.

**Welche der vier Textzeilen steuert den Roboter zum unbekannten Objekt?**

- A) Ha' poS poS Ha' Ha' nIH
- B) Ha' Ha' poS Ha'
- C) Ha' poS poS Ha' nIH Ha'
- D) Ha' poS nIH vl'ogh Ha' poS



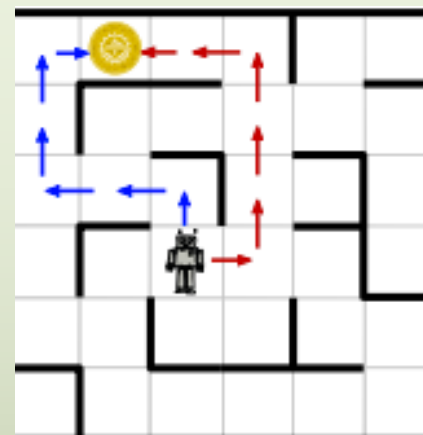
**Antwort A ist richtig:**

Keine der durch die Textzeilen gegebenen Befehlsfolgen enthält mehr als sechs Befehle. Mit jedem Befehl kann der Roboter einen Schritt in ein benachbartes Quadrat machen. Das Bild zeigt die beiden Wege, die den Roboter in sechs Schritten zum Objekt führen.

Die Befehlsfolge muss also den Roboter entweder so steuern (rote Pfeile):

**rechts, vor, vor, vor, links, links.** Dazu passt keine der vier Textzeilen. Oder die Befehlsfolge muss den Roboter so steuern (blaue Pfeile):

**vor, links, links, vor, vor, rechts.** Dazu passt nur Textzeile A) mit Ha' = vor, poS = links und nIH = rechts.



### Webseiten und Stichwörter

Kryptoanalyse, Kryptologie

- <http://de.wikipedia.org/wiki/Kryptoanalyse>

## Dies ist Informatik!

Kryptoanalyse ist die Wissenschaft des Lesens verschlüsselter Botschaften. Seit der Antike versuchen Kryptoanalytiker geheime Nachrichten zu entschlüsseln. Dabei wird auch das Wissen über die mögliche Bedeutung der verschlüsselten Botschaften verwendet. Als im Zweiten Weltkrieg versucht wurde, die von der Enigma-Maschine verschlüsselten Botschaften zu entschlüsseln, suchte man gezielt nach deutschen Städtenamen und nach Wörtern, die in Wetterberichten vorkommen. Denn wichtige Nachrichten begannen oft mit einer Wettervorhersage. Bei dieser Biber-Aufgabe konntest du dich als Kryptoanalytikerin oder Kryptoanalytiker betätigen. Die Entschlüsselung ist übrigens wesentlich einfacher, wenn man klingonisch spricht.

# Vielen Dank



**INFORMATIK-BIBER SCHWEIZ  
CASTOR INFORMATIQUE SUISSE  
CASTORO INFORMATICO SVIZZERA**



**INFORMATIK-BIBER SCHWEIZ  
CASTOR INFORMATIQUE SUISSE  
CASTORO INFORMATICO SVIZZERA**